

Exhibit A



UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

UNITED STATES OF AMERICA,

Criminal No. 2:16cr104

v.

LARRY JAMES REECE, II,

Defendant.

ORDER

Pending before this Court is a Motion to Suppress brought by Defendant Larry James Reece, II. ECF No. 21. A hearing on the Motion was convened on January 11, 2017. For the reasons contained herein, the Court finds that the warrant was unsupported by probable cause. The Court also determines that the “good faith exception” to the exclusionary rule is inapplicable. Accordingly, the Court is compelled to **GRANT** the Motion to Suppress.

I. BACKGROUND

A. Procedural Background

On October 28, 2015, investigators learned that an IP address was used to “download, and/or attempt to download” a video of child pornography. On December 15, 2015, a subpoena from the United States Department of Justice was issued to Cox Communications requesting the subscriber information associated with the IP address that was used on October 28, 2015 to “download” or “attempt to download” the child pornography. Cox Communications provided the requested business records on January 6, 2016. The records indicated that the account linked to the IP address at issue was associated with Defendant.

On April 5, 2016, Harald S. Julsrud, a Special Agent for the Child Exploitation and National Security Investigations Unit of Homeland Security Investigations-Norfolk, applied for a search warrant of Defendant's residence based upon the attempted download of child pornography on October 28, 2015. A federal Magistrate Judge reviewed the warrant application and the affidavit filed in support, and the Magistrate Judge signed the search warrant on the application date of April 5, 2016. The search warrant was executed without notice (as a "no-knock" warrant) at Defendant's home on April 15, 2016. During the search, law enforcement officers seized numerous electronic media, including images of child pornography. Defendant challenges the validity of the warrant.

B. The Warrant and Affidavit

The affidavit in support of the search warrant is fourteen pages long, but contained only two paragraphs that describe facts and details specific to Defendant. The majority of the affidavit consisted of generalized allegations reviewing: (1) the qualifications and experience of the affiant, Special Agent Julsrud; (2) passages from the "pertinent federal criminal statutes," 18 U.S.C. §§ 2252(a)(2) and (a)(4); (3) definitions of various key terms and descriptions of the investigative process; (4) descriptions of the characteristics of child pornography collectors; and (5) facts regarding the background investigation, certain websites (addressed more fully herein), and the use of file sharing services ("FSS"). Aff., ECF No. 26-3.

With regard to Defendant, the affidavit alleged that on October 28, 2015, an IP address associated with Defendant "was used to download, and/or attempt[] to download, file content" that was associated with a Uniform Resource Locator ("URL") consisting of a 49-second video file "depicting what appears to be an adult male from the waist down, with his pants pulled down and with an erect penis, and the lower back and buttocks of what appears to be a minor, engaging

in sexual intercourse (either actual or simulated) until the adult male ejaculates on the apparent minor's back and buttocks." Aff., ECF No. 26-3, ¶ 47.

The affidavit alleged only that Defendant's IP address was used to navigate to a website with a link to a video of child pornography. The video file containing the child pornography was encrypted, requiring a password to download and view the video.

C. "The Network," "Bulletin Board A," and "The File Sharing Service"

The affidavit explains three web-based services: "The Network," "Bulletin Board A," and "The File Sharing Service" (FSS).¹ These can be used to facilitate access to, and the accumulation of, child pornography.

"The Network" is a specially designed network that enables anonymous communication over the Internet. Users can access The Network only through a specialized internet browser, which serves as a gateway to content configured to be available only through The Network. The browser is publicly available, but users must seek it out and download it. Because of this, The Network is accessible only to individuals who actively seek it out, and inadvertent access is highly unlikely.

"Bulletin Board A" is a website dedicated to the advertisement and distribution of child pornography. Bulletin Board A operates on The Network, and is accessible only to Internet users who have downloaded The Network. There are 1,500 "users" of Bulletin Board A. Users of Bulletin Board A post new content and engage in discussions involving the sexual exploitation of minors.

Bulletin Board A contains a number of bulletin boards, organized by categories and sub-categories of child pornography, where users can post text, preview images, and links to child pornography. The links posted on Bulletin Board A generally lead a user to an image or video

¹ These are stand-in terms, used to protect ongoing investigations into these services.

file stored on an external cloud-based service, where the user can download the content sought. These external cloud-based services are not part of Bulletin Board A; they are external websites that can be accessed on the “ordinary Internet” and may also host innocent content.

Although Bulletin Board A operates on The Network, many of the external websites that can be accessed via Bulletin Board A can also be accessed directly through the Internet. Some websites containing child pornography that are posted on Bulletin Board A can be accessed without clicking on the links found on Bulletin Board A.

On October 26, 2015, investigators observed a posting on Bulletin Board A titled “Hot latin doggyfuck,” followed by a preview still image file containing several smaller still images from the referenced video. The posting also included a link (with the URL relevant in this case) and a password that was required to download and view the file. If a user clicked on the link above, he or she would be redirected to an external file-sharing website (“FSS”) that operated on the Internet. If the user entered the required password, he or she could download a 49-second video depicting child pornography.

On October 28, 2015, an IP address associated with Defendant was used to “download and/or attempt to download” file content associated with the link above. Aff., ECF No. 26-3, ¶ 47. This evidence indicates that Defendant (or someone associated with Defendant’s IP address) clicked on a link to a video of child pornography. That link was posted on Bulletin Board A, and redirected users to an external file-sharing website (“FSS”) that operated on the Internet.

D. Suppression Motion

As noted, the link referenced above could be accessed through Bulletin Board A, which contained a post with the link to the external website where the video file could be found. The affidavit did not allege that Defendant visited Bulletin Board A, or clicked on a link posted on

Bulletin Board A, or was one of the 1,500 “approved users” of Bulletin Board A. The affidavit did not state how Defendant (or the person associated with his IP address) found or navigated to the link to the illicit video. The affidavit also failed to allege whether the video was downloaded successfully by Defendant’s IP address,² and failed to allege whether the illicit nature of the video’s content was apparent before viewing the video. The affidavit alleged only that Defendant’s IP address was used to access—or attempt to access—a link to a video of child pornography.

Defendant moves to suppress all evidence seized in the search of his home on April 15, 2016. He argues that the search warrant of his home was issued in violation of the Fourth Amendment to the United States Constitution for the following reasons: (1) the search warrant was unsupported by probable cause; (2) the search warrant was issued based on stale evidence; and (3) the search warrant was supported by an affidavit that was tainted by the material omission of important facts, thereby justifying a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978).³

The Government argues that the warrant was obtained and executed validly. The Government also argues alternatively that the “good faith exception” to the exclusionary rule should apply under the circumstances presented.

After careful consideration of the arguments presented and the applicable law, this Court concludes that the warrant at issue lacked sufficient probable cause and was supported by

² The video file was password-protected. Aff., ECF No. 26-3, ¶ 40. The affidavit omitted the fact that there is no evidence that the person using Defendant’s IP address on October 28, 2015, ever entered a password to access the video.

³ In *Franks*, the United States Supreme Court held that when a defendant makes a substantial preliminary showing that the police procured a warrant to search the defendant’s property with deliberate or reckless misrepresentations in the warrant affidavit, and that the misrepresentations had been necessary to the finding of probable cause, the Fourth Amendment to the Constitution entitles the defendant to an evidentiary hearing to determine whether the warrant was invalid. *Franks*, 438 U.S. at 155–56.

evidence that was stale. After further scrutiny, the Court also determines that the exclusionary rule cannot be avoided pursuant to the “good faith exception.”

II. STANDARDS OF LAW

The Fourth Amendment to the United States Constitution provides that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. Amend. IV. The Supreme Court of the United States reasoned in *Illinois v. Gates* that “probable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.” 462 U.S. 213, 232 (1983).

“[T]he task of the reviewing court is not to conduct a *de novo* determination of probable cause, but only to determine whether there is substantial evidence in the record supporting the magistrate’s decision to issue the warrant.” *Massachusetts v. Upton*, 466 U.S. 727, 728 (1984). “When reviewing the probable cause supporting a warrant, a reviewing court must consider only the information presented to the magistrate who issued the warrant.” *United States v. Wilhelm*, 80 F.3d 116, 118 (4th Cir. 1996) (citing *United States v. Blackwood*, 913 F.2d 139, 142 (4th Cir. 1990)).

III. ANALYSIS

A. Probable Cause

Probable cause is not subject to a precise definition. See *United States v. Allen*, 631 F.3d 164, 172 (4th Cir. 2011); see also *United States v. Martin*, 426 F.3d 68, 76 (2d Cir. 2005) (citing *United States v. Leon*, 468 U.S. 897, 958 (1984)). A magistrate considering whether probable

cause supports the issuing of a search warrant must “make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the ‘veracity’ and ‘basis of knowledge’ of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Gates*, 462 U.S. at 238.

For a magistrate to conclude that probable cause exists, a warrant application’s supporting affidavit must be more than conclusory. The affidavit “must provide the magistrate with a substantial basis for determining the existence of probable cause.” *Id.* at 239. When examining an affidavit, a magistrate may rely on representations from law enforcement officers. These officers may “draw on their own experience and specialized training to make inferences from and deductions about the cumulative information available to them that might well elude an untrained person,” as long as the affidavit contains facts to support the law enforcement officers’ conclusions. *United States v. Johnson*, 599 F.3d 339, 343 (4th Cir. 2010) (quoting *United States v. Arvizu*, 534 U.S. 266, 273 (2002)); *see also United States v. Brown*, 958 F.2d 369 (Table), 1992 WL 46838, at *5 (4th Cir. Feb. 12, 1992) (noting that “magistrates, in making probable cause determinations, may rely upon an experienced police officer’s conclusions as to the likelihood that evidence exists and where it is located.”).

A magistrate’s determination of probable cause is afforded great deference by a court reviewing a warrant. *See Gates*, 462 U.S. at 236. The duty of a reviewing court “is simply to ensure that the magistrate had a ‘substantial basis for . . . conclud[ing] that’ probable cause existed.” *Id.* at 238–39 (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)); *see also United States v. Blackwood*, 913 F.2d 139, 142 (4th Cir. 1990). A reviewing court should “resist

the temptation to ‘invalidate warrant[s] by interpreting affidavit[s] in a hypertechnical, rather than a commonsense, manner.’” *Blackwood*, 913 F.2d at 142 (quoting *Gates*, 462 U.S. at 236).

Defendant argues that the search warrant in this case was unsupported by probable cause because it failed to establish with sufficient likelihood that Defendant accessed Bulletin Board A. Defendant argues that the warrant application contains a single allegation that on one occasion the IP address associated with Defendant was used to access a link (bearing the relevant URL) to a video of child pornography.

Although the warrant application contained extensive background information about Bulletin Board A, it failed to allege that Defendant ever visited Bulletin Board A. Defendant also argues that the affidavit failed to provide any facts connecting Defendant’s IP address to Bulletin Board A, aside from the fact that the link above was posted on Bulletin Board A. Defendant asserts that “the fact that someone using [Defendant’s] IP address attempted to access the URL of a popular file sharing service, which itself bore no indicia of child pornography, does not provide probable cause to search [Defendant’s] home.” ECF No. 21 at 10.

According to the affidavit, a file-sharing site (“FSS”) provided records associated with a unique URL that led to a video containing child pornography. Aff., ECF No. 26-3, ¶ 46. “On October 28, 2015, . . . [Defendant’s] IP address . . . was used to download, and/or attempted to download, file content associated with that URL,” and that content consisted of a 49-second video depicting child pornography. Aff., ECF No. 26-3, ¶ 47. The affidavit contains no other facts or information specific to Defendant or his IP address.

At the January 11, 2017 evidentiary hearing, the affiant and executing officer, Special Agent Julsrud, acknowledged that at the time the affidavit was presented, there was no evidence that Defendant had ever accessed Bulletin Board A. Supp. Hrg. Tr., 54: 16-18 (Jan. 11, 2017)

(Q: “And there’s no evidence he went to Bulletin Board A, correct?” Special Agent Julsrud: “No.”). Special Agent Julsrud also testified that the only way a person would have known that the listed URL was a link to child pornography would have been if that person went to Bulletin Board A and saw the accompanying description. *Id.* at 54: 13–15 (Jan. 11, 2017) (Q: “The only way a person would have known that it was child pornography is if [the person] went to Bulletin Board A?” A: “Yes. At that time, yes.”).

Scrutiny of the affidavit and of Special Agent Julsrud’s subsequent testimony provides scant evidence to support an inference that Defendant accessed Bulletin Board A. An IP address associated with Defendant either downloaded or attempted to download file content that contained child pornography. Defendant, or someone with access to his IP address, clicked on a link—with an innocuous URL address—that could have been accessed through Bulletin Board A (where the link posted) or through other means. *See* Supp. Hrg. Tr., 43: 20–23 (Jan. 11, 2017) (Q: “[Y]ou certainly knew at the time that you started this investigation that [the URL] could have come from somewhere other than Bulletin Board A?” A: “It was a possibility, yes.”); *Id.* at 55: 17–20 (Q: “So, therefore, if a regular person is looking at that URL or reading it, [the person] would not know that it pertained to child pornography, correct?” A: “No.”).

The decisions in *United States v. Falso*, 544 F.3d 110 (2d Cir. 2008) and *United States v. Coreas*, 419 F.3d 151 (2d Cir. 2005) are instructive regarding the determination of probable cause. In *Falso*, the United States Court of Appeals for the Second Circuit found that an affidavit alleging that a defendant “appear[ed]” to “have gained or attempted to gain” access to a website that distributed child pornography and had been convicted of misdemeanor sexual abuse of a minor eighteen years earlier was insufficient to establish probable cause. 544 F.3d at 112.

In the absence of other factors⁴ weighing in favor of a determination of probable cause, “membership in or subscription to a child-pornography website is an important consideration . . . because it supports the ultimate inference . . . that illegal activity is afoot.” *Id.* at 121.

Here, the affidavit lacked factual assertions that Defendant subscribed to or accessed a child pornography website. The affidavit supported only an inference that Defendant clicked on a link to an illicit video that *could have* been accessed through a child pornography website (Bulletin Board A). That the link to the illicit video *could be accessed* via Bulletin Board A is insufficient to support the resulting search without the Court making the “inferential leap” that Defendant *must have accessed* Bulletin Board A to navigate to the illicit material. *See id.* at 124.

In *Coreas*, the Second Circuit held that probable cause was not established by an allegation that a defendant logged onto a website containing child pornography and then joined an e-group by the single click of his mouse. 419 F.3d at 156. “The notion that, by this act of clicking a button, [the defendant] provided probable cause for the police to enter his private dwelling and rummage through his personal effects seems utterly repellent to core purposes of the Fourth Amendment.” *Id.*

Similarly, the affidavit at issue here relies upon one click of a mouse: Defendant allegedly clicked on a link to an illicit video containing child pornography. That link was posted

⁴ According to the Second Circuit, “[t]he common thread among these cases is the defendant’s membership in or subscription to websites whose principal purpose was the collection and/or sharing of child pornography.” *Id.* at 120. Additional factors include: (1) acts of the defendant that tend to negate the possibility that his membership or subscription was unintended, such as evidence of access to or membership in multiple sites, or evidence that the defendant entered credit card or other personal information; (2) email addresses or screennames suggestive of an interest in collecting child pornography; and (3) the defendant’s criminal history relating to child pornography. *Id.*

on Bulletin Board A. Absent evidence that Defendant accessed Bulletin Board A, it is possible that the link could have been accessed through innocent means.⁵

The Government cites *United States v. Ramsburg*, 114 Fed. App'x 78 (4th Cir. 2004) in support of the assertion that probable cause may exist where there is an allegation of the transmission of a single image. In *Ramsburg*, the affidavit at issue contained the following allegations: (1) the defendant was a member of two online child pornography websites; (2) the defendant received 178 images of child pornography; and (3) an email address registered to the defendant transmitted an illicit image to an agent. Despite the subsequent invalidation of the allegation involving 178 images, the Fourth Circuit determined that the affidavit's remaining allegations supported a finding of probable cause.

Here, there are no allegations of membership in a child pornography website or transmission or receipt of child pornography. The relevant allegation in this case is that Defendant "download[ed] and/or attempted to download" file content from the relevant URL that consisted of an illicit video.

Defendant also argues persuasively that, absent some evidence of "collecting behavior," evidence of an isolated and possibly unsuccessful attempt to access an illicit video over five months earlier is too stale to establish sufficient probable cause to search Defendant's home. Defendant was alleged to have "download[ed] and/or attempted to download" the illicit video on October 28, 2015. The search warrant was signed on April 5, 2016.

The Court acknowledges that the Department of Justice issued a subpoena to Cox Communications requesting the subscriber information associated with the relevant IP address on December 15, 2015. However, Cox Communications provided business records on January

⁵ The Court notes the distinction that the defendant in *Coreas* accessed a website that was a known source of child pornography. In this case, whether Defendant ever accessed a website that clearly promoted or depicted child pornography was never established, and remains unclear.

6, 2016, and the warrant application was not made until April 5, 2016—three months after the records were obtained and over five months after the download attempt.

Challenges of staleness have been addressed generally by the Fourth Circuit:

In the context of child pornography cases, courts have largely concluded that a delay—even a substantial delay—between distribution and the issuance of a search warrant does not render the underlying information stale. This consensus rests on the widespread view among the courts . . . that *collectors and distributors* of child pornography value their sexually explicit materials highly, rarely if ever dispose of such material, and store it for long periods in a secure place, typically in their homes.

United States v. Richardson, 607 F.3d 357, 370 (4th Cir. 2010) (emphasis added).

In cases in which a defendant’s staleness challenge has been rejected, the warrant affidavits have contained allegations that the defendant either distributed child pornography or exhibited “collector behavior.” *Id.* at 363 (holding that a four-month time period between the defendant’s alleged transmission of child pornography and the issuance of the search warrant did not preclude a finding of probable cause based on staleness, because of the existence of “allegations specifically related to [the defendant] *and* the ‘general profile’ of child pornographers”) (emphasis added); *United States v. Sassani*, 139 F.3d 895 (Table), 1998 WL 89875, at *5 (4th Cir. March 4, 1998) (upholding a search warrant with a six-month lapse based on the finding that evidence of the “*distribution* of child pornography on several different occasions may provide sufficient probable cause despite delay between a distribution and the date a search warrant is sought or executed”) (emphasis added); *see also United States v. Davis*, 313 F. App’x 672 (Table), 2009 WL 489998, at *1 (4th Cir. Feb. 27, 2009) (recognizing circuits that have found that child pornographers *who are collectors* keep their contraband for a long time, and that information that is a year old is not stale as a matter of law in such cases).

Federal courts may infer that a suspect is a “collector” of child pornography based on factors such as the following: (1) a suspect’s admission of being a pedophile or other evidence that would corroborate this fact; (2) a suspect’s extended history of possessing or receiving pornography images; or (3) an allegation that a suspect paid for access to child pornography. *United States v. Raymonda*, 780 F.3d 105, 114–15 (2d Cir. 2015). Courts have also inferred that a suspect is a collector of child pornography on the basis of a single allegation of possession or receipt where “the suspect’s access to the pornography images depended on a series of sufficiently complicated steps to suggest his willful intention to view the files,” or where the defendant subsequently redistributed the pornographic material to other users. *Id.* at 115.

The search warrant and supporting affidavit presented here failed to allege that Defendant distributed child pornography, or that he possessed any traits or characteristics associated with “collectors” of child pornography. Also, the allegation that Defendant accessed the link to the illicit video is unaccompanied by any evidence that Defendant engaged in a series of complicated steps to view the illicit video. This lack of evidence diminishes the bases upon which staleness can be excused. *Id.* (citing *United States v. Vosburgh*, 602 F.3d 512, 528 (3d Cir. 2010)). Evidence of a single attempt to access child pornography, “absent any other circumstances suggesting that the suspect accessed [the child pornography] deliberately or ha[d] a continuing interest in child pornography, fails to establish probable cause that the suspect will possess illicit images many months later.” *Id.* at 109.

As acknowledged above, a finding of probable cause “may rely upon an experienced police officer’s conclusions as to the likelihood that evidence exists and where it is located.” *United States v. Brown*, 958 F.2d 369 (Table), 1992 WL 46838, at *5 (4th Cir. Feb. 12, 1992); *see also Richardson*, 607 F.3d at 361. However, the affidavit must also be supported by specific

and articulable facts and inferences that can be drawn from the affiant's training and experience. *See Illinois v. Gates*, 462 U.S. 213, 273 (1983). Those specific and articulable facts are absent in this case. *See, e.g., Richardson*, 607 F.3d at 361 (where the affidavit in support of probable cause relied upon the officer's training and experience, and also alleged that the defendant sent two email messages containing illicit images, and that the defendant was a registered sex offender with two prior convictions involving minors).

After considering Defendant's well-taken arguments regarding staleness and the paucity of factual allegations linking this Defendant to the act of viewing and collecting or distributing child pornography, this Court concludes that the search warrant was not supported by probable cause. For the following reasons, the Court also determines that the "good faith exception" to the exclusionary rule is inapplicable.

B. Good Faith Exception

Generally, if a search violates the Fourth Amendment, "the fruits thereof are inadmissible under the exclusionary rule, a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect." *United States v. Doyle*, 650 F.3d 460, 466 (4th Cir. 2011) (citing *United States v. Calandra*, 414 U.S. 338, 348 (1974)) (internal quotations omitted). However, because exclusion is so drastic a remedy, it represents a "last resort." *United States v. Stephens*, 764 F.3d 327, 335 (4th Cir. 2014).

The Supreme Court established the good faith exception to the exclusionary rule in *United States v. Leon*, 468 U.S. 897, 922 (1984). Under this exception, courts may decline to exclude evidence obtained pursuant to a later-invalidated search warrant if law enforcement's reliance on the warrant was objectively reasonable. *Doyle*, 650 F.3d at 467.

When considering the application of the good faith exception, courts are “not limited to consideration of only the facts appearing on the face of the affidavit.” *Id.* at 471 (internal citation omitted). Instead, courts must “examine the totality of the information presented to the magistrate in deciding whether an officer’s reliance on the warrant could have been reasonable.” *United States v. Legg*, 18 F.3d 240, 244 n.1 (4th Cir. 1994).

There are four circumstances in which the good faith exception is inapplicable:

(1) if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth; (2) if the issuing magistrate wholly abandoned his judicial role in the manner condemned in *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319 (1979); (3) if the affidavit supporting the warrant is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) if under the circumstances of the case the warrant is so facially deficient – i.e., in failing to particularize the place to be searched or the things to be seized – that the executing officers cannot reasonably presume it to be valid.

Doyle, 650 F.3d at 467 (citing *United States v. DeQuasie*, 373 F.3d 509, 519–20 (4th Cir. 2004) (quoting *Leon*, 468 U.S. at 923)).

Defendant argues in part that the good faith exception is inapplicable because the issuing Magistrate wholly abandoned his detached and neutral judicial role (“prong two”). Defendant also contends that the issuing Magistrate was misled by the inclusion of knowingly or recklessly false information (“prong one”).

The Court rejects summarily Defendant’s “prong two” argument before evaluating the “prong one” assertions involving misleading and reckless aspects of the affidavit at issue. To prove that the Magistrate abandoned his judicial role as required in “prong two,” Defendant must allege objective facts to show that the Magistrate no longer acted as a judicial officer. For example, in *Lo-Ji Sales*, the Magistrate took on the role of a law enforcement officer when he

became a member and leader of the police search party that seized the evidence in question. 442 U.S. at 327. Such is clearly not the case here.

Defendant also contends that the issuing Magistrate was misled by the inclusion of knowingly or recklessly false information in the affidavit, and by the knowing or reckless omission of material information from the affidavit (“prong one”). Defendant’s arguments concerning the misleading nature of the affidavit require closer examination.

As noted, the good faith exception is inapplicable—and suppression is warranted—“if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth.” *Doyle*, 650 F.3d at 467 (internal citations omitted). “[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence.” *Herring v. United States*, 555 U.S. 135, 144 (2009). “To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system.” *Id.* Overall, “the exclusionary rule is applicable ‘when police exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights, [and] the deterrent value of exclusion is strong and tends to outweigh the resulting costs.’” *United States v. Stephens*, 764 F.3d 327, 336 (4th Cir. 2014) (citation omitted).

In *Herring*, the United States Supreme Court considered whether, and under what circumstances, evidence should be suppressed when police commit constitutional errors in obtaining such evidence. In that case, police officers conducted a search based on incorrect information provided by another police department regarding an alleged outstanding warrant for the defendant’s arrest. The Supreme Court held that the good faith exception applied because

suppression of the evidence would have only a “marginal deterrent effect on police behavior,” since the violation arose out of “isolated negligence attenuated from the arrest, rather than systemic error or reckless disregard of constitutional requirements.” *Herring*, 555 U.S. at 147, 137.

In so holding, the Supreme Court established a balancing test whereby the exclusionary rule “applies only where its deterrent effect outweighs the substantial cost of letting guilty and possibly dangerous defendants go free.” *Id.* at 141. Put differently, the exclusionary rule “applies only where it results in appreciable deterrence.” *Leon*, 468 U.S. at 909. To the extent that the application of the exclusionary rule could provide marginal or incremental deterrence, this possible benefit must be outweighed by its substantial social costs. *Herring*, 555 U.S. at 141 (internal citations omitted). The Supreme Court reasoned that “the question turns on the culpability of the police and the potential of exclusion to deter wrongful police conduct.” *Id.* at 137. The good faith exception applies to errors that arise from nonrecurring and attenuated negligence on the part of the police, as opposed to intentional or culpable conduct. *Id.* at 144.

The Supreme Court provided two examples of police misconduct that would warrant the exclusionary remedy: a police department’s systemic recklessness in maintaining a warrant system; or “knowingly ma[king] false entries to lay the groundwork for future false arrests.” *Id.* at 146. The Supreme Court emphasized that the exclusionary rule applies typically in cases like *Mapp v. Ohio*, in which police engaged in “flagrant or deliberate violation of rights.” *See id.* at 144 (citing *Mapp v. Ohio*, 367 U.S. 643, 644-45 (1961) (holding that exclusion of improperly obtained evidence was appropriate in a case in which officers forced open the door to the defendant’s home, prevented her lawyer from entering, brandished a false warrant, and forced the defendant into handcuffs while they searched her home for obscenity)).

To challenge a search warrant on the theory that it contains misleading information or omits material facts, a defendant must show: (1) that the affiant deliberately or recklessly included inaccurate information or omitted material facts from the affidavit; and (2) given the totality of the circumstances, that the errors and/or omissions in the affidavit are critical to the finding of probable cause and the decision to issue the search warrant. *United States v. Doyle*, 650 F.3d 460, 469 (4th Cir. 2011); *United States v. Andrews*, 577 F.3d 231, 238–39 (4th Cir. 2009); *see also United States v. Jones*, 200 Fed. App'x 229, 2006 WL 2668826, at *2 (4th Cir. Sept. 18, 2006).

After *Herring*, the United States Court of Appeals for the Fourth Circuit has applied the exclusionary rule—and found the good faith exception to be inapplicable—in limited situations. In *Edwards*, police officers discovered contraband in the defendant's underwear, and subsequently violated the defendant's constitutional rights when they retrieved the contraband in a “dangerous manner.” *United States v. Edwards*, 666 F.3d 877, 885 (4th Cir. 2011). The court found that suppression was warranted because the circumstances of the unconstitutional search were likely to recur, and “the interests of deterrence . . . are advanced by discouraging the routine use of dangerous procedures [of the type in this case].” *Id.* at 886–87 (citing *Davis v. United States*, 564 U.S. 229, 236–37 (2011) (holding that the “sole purpose” of the exclusionary rule “is to deter future Fourth Amendment violations.”)).

In *Rush*, a police officer knowingly lied to the defendant by claiming falsely that he had a warrant to search the apartment where the defendant was staying. *United States v. Rush*, 808 F.3d 1007, 1008 (4th Cir. 2015). The Fourth Circuit held that suppression was warranted—and the good faith exception was inapplicable—because the police misconduct in this situation rose above negligence or reasonable reliance on faulty information.

Here, Defendant contends that the Magistrate was misled by the inclusion of knowingly or recklessly false information, and by the knowing or reckless omission of material information in the affidavit.⁶ The arguments advanced for rejecting the good faith exception to the exclusionary rule presented a profoundly difficult challenge for the Court. The conduct undertaken in drafting the warrant application exceeds only marginally the kind of nonrecurring and attenuated negligence by law enforcement officials that supports the application of the good faith exception. However, after careful scrutiny and evaluation, the Special Agent's conduct here—when coupled with the likely recurrence of systemic errors or confusion in similar investigations in the future—is deemed sufficient to compel suppression.

1. Careless Drafting of the Affidavit

The conclusion of the affidavit at issue asserted that the user at the subject premises “received or attempted to receive, possessed and/or accessed with intent to view child pornography via the listed *email account*.” Aff., ECF No. 26-3, ¶ 55 (emphasis added). The Government agrees that this is false. The warrant was supported by evidentiary references to Defendant's IP address, not his email account.

Special Agent Julsrud explained this mistake as a “typographical error.” Supp. Hrg. Tr., 75: 1-4. Further, on cross-examination, he admitted that he did not review the final paragraph.

⁶ Defendant asserts that the good faith exception must be inapplicable for the following reasons: (1) Defendant's “email account” instead of his “IP address” was referenced incorrectly as being at issue in the affidavit's conclusion; (2) the affidavit emphasized facts about child pornography in general (such as extensive information about The Network and Bulletin Board A), while failing to acknowledge the absence of evidence connecting Defendant to these known child pornography sources; (3) the affidavit's inclusion of extensive details about the characteristics of child pornography collectors, in the absence of an acknowledgment that there is no evidence that Defendant shares any of these characteristics; (4) the affidavit's implications that Defendant successfully downloaded the illicit video, and entered a password to do so, despite the lack of evidence confirming this; (5) the affiant's inaccurate testimony presented at the subsequent evidentiary hearing regarding the existence of additional evidence the affiant may have possessed before applying for the warrant application; and (6) the reckless manner in which the search warrant was executed.

Id. at 115:5-6 (Q: “And did you review that paragraph?” A: “Apparently not.”). Such an error, while unlikely to have affected the determination of probable cause, suggests a troublingly reckless approach to the preparation and submission of the warrant application. Such errors may also be indicative of larger, systemic flaws in the guidance provided for these kinds of investigations.

2. The Misleading Nature of the Affidavit’s Contents

Extensive information about law enforcement’s background investigation into Bulletin Board A, and how members of that entity use file sharing services, was detailed in the affidavit. There is no evidence that Defendant was a member of Bulletin Board A or ever accessed it. The affidavit omitted this fact. The affidavit’s failure to address the absence of any connection between Bulletin Board A and Defendant’s known characteristics rendered this extensive information misleading. The nature of this flaw, and the likelihood of its repetition, is perhaps the most troubling to the Court.

The affidavit also carefully reviewed the general characteristics shared by collectors of child pornography. Yet (in direct contravention of the explicit directive provided in a guidelines template, addressed below), the affidavit failed to present any factual allegations or evidence that Defendant possesses any of these characteristics. Including “collector” language without particularizing such information to an individual defendant can lead to recklessly misleading results. In this case, the inclusion of “collector” language was reckless because there was no evidence that Defendant possessed any traits or characteristics of a child pornography “collector.” The inclusion of “collector” language was material to the probable cause determination. The absence of clarifying information that either tailored “collector” characteristics to Defendant or acknowledged the lack of such connections, was, therefore

reckless. In the absence of a clarification that no such evidence was found, it was reasonable for the Magistrate Judge to infer that Defendant may have fit the profile of a “collector” of child pornography.

Moreover, the affidavit stated that the illicit video was password-protected. Aff., ECF No. 26-3, ¶ 40. Special Agent Julsrud later testified that he knew that there was no evidence that Defendant had entered a password to download or view the illicit video. Supp. Hr’g Tr. 112: 17-19. This knowledge was omitted from the affidavit, however. Without this disclosure, the affidavit’s references to passwords gave rise to a reasonable (and misleading) inference that Defendant entered a password—and engaged in an additional step—to attempt to view the illicit video. In light of the totality of the circumstances and Special Agent Julsrud’s knowledge that there was no evidence that a password was entered, this information must be deemed as recklessly omitted. The omission likely contributed to a finding of probable cause, and the practice of omitting such essential information suggests systemic flaws in how these sensitive investigations are undertaken.

Taking into consideration the totality of the circumstances, these errors were material to the probable cause determination made in this case. They are also indicative of a reckless disregard for accuracy, and suggest a likelihood of recurrences in future investigations.

3. Other Indicia of Recklessness

Agent Elizabeth De Jesus of the Cyber Crimes Center testified that Special Agent Julsrud was provided with assistance in preparing the warrant application and affidavit. Specifically, a “template” that could be particularized to this investigation was provided to assist in drafting the warrant and affidavit. Supp. Hr’g Tr. 58: 20-21; 59: 2-4 (Q: “[W]hat, in particular, is in the template?” A: “Well it’s a template that would pertain to the leads that we’re sending out, not

someone specific. They can edit it as it pertains to their specific subscriber.”). She further testified that Special Agents are directed to edit the template to tailor the application to the particular defendant under investigation. *Id.* at 61: 22-24 (Q: “So you would then rely on the agents to take out information that’s irrelevant?” A: “Correct.”).

The template provided to Special Agent Julsrud contained an explicit directive regarding when to include language about the characteristics of “collectors” of child pornography. *See* ECF No. 41, Ex. B, ¶ 30 (“NOTE: Use this language ONLY if the target fits the profile and you are comfortable with stating it based on your experience with these cases. CRITICAL: you must tie these characteristics to the specific offender. Because this operation encompasses a wide range of conduct please go through and modify language for your particular offender.”).

Despite this directive, and in direct contradiction to it, Special Agent Julsrud included “collector” language in his affidavit without particularizing this information to Defendant. He admitted that he includes “collector” language in all of his child pornography warrant applications. Supp. Hr’g. Tr. 76: 24-77:2.

Regarding this aspect of his preparation in this case, Special Agent Julsrud explained that he declined to strictly follow the template provided to assist his warrant application.⁷ Instead, he used a “go-by” of applications and affidavits, which he described as being more common when drafting affidavits in this district. Special Agent Julsrud testified that he adapted the “go-by” to fit the facts of this particular case. *Id.* at 76:1-6.

Notwithstanding the testimony from Agent DeJesus and from Special Agent Julsrud about the processes undertaken for investigating and drafting the warrant application in this case, the Court is compelled to acknowledge other misleading or confusing aspects of Special Agent Julsrud’s testimony. At the January 11, 2017 evidentiary hearing, Special Agent Julsrud’s

⁷ Agent De Jesus also testified that agents are not required to use the template. *Id.* at 65:25; 66: 1-2.

testimony about his execution of the search warrant was misleading. He initially testified that he believed that he had applied for a no-knock warrant. *Id.* at 96: 2-3. He later changed his testimony to state that he did not specifically ask for a no-knock warrant in this case. *Id.* at 117: 2-4.

Special Agent Julsrud also testified that Agent De Jesus told him, via email, that the only way to access the URL at issue was through Bulletin Board A. Supp. Hr’g Tr. 94: 21-25; 95: 1. However, this critical testimony was never corroborated, because the alleged email was never provided.⁸

The Court notes further that Special Agent Julsrud testified that he was aware of two additional “leads” concerning Defendant when he prepared his application for the search warrant. *Id.* at 82: 22-24. After the hearing, he filed an affidavit clarifying that he was aware of only one additional “lead” prior to applying for the search warrant. ECF No. 35-1 at 2-3.

Special Agent Julsrud testified that he did not purposely or intentionally try to mislead the Magistrate Judge. *See id.* at 75: 1-9; 79: 19-21. However, the Court is compelled to find—after considering the totality of the circumstances—that these errors in his testimony support a conclusion that the process undertaken in this warrant application reflects a reckless disregard for accuracy that was material to the probable cause determination. This Court must conclude that suppression is warranted—and the good faith exception is inapplicable—because the flaws existing in the warrant and supporting affidavit go beyond nonrecurring or attenuated negligence and are not the result of an officer’s reasonable reliance on faulty information.

⁸ Agent De Jesus also testified about the connection between Bulletin Board A and the URL at issue in this case. Agent De Jesus explained that the information provided to Special Agent Julsrud was that the URL had been posted on Bulletin Board A and had not been found anywhere else. Supp. Hr’g Tr. 50: 2-7. After the warrant in this case had been issued, agents were advised that the URL at issue could have been accessed through innocent means. *Id.* at 46: 2-5. This confusion may have contributed to the misleading aspects of the affidavit regarding Bulletin Board A.

4. Concerns Regarding the Likelihood of Recurring Systemic Errors

The question of whether to invoke the good faith exception and decline to suppress the evidence seized in this case is close, and the Court's decision is difficult. However, the Court's interests in deterring future constitutional violations and upholding the core purposes of the exclusionary rule tip the scales in favor of suppression.

As referenced in Footnote 8 above, Agent De Jesus testified that Special Agent Julsrud had been advised that the URL had been posted on Bulletin Board A and had not been found anywhere else. Supp. Hr'g Tr. 50: 2-7. She explained that agents were advised that the URL at issue could have been accessed through innocent means, but that this information was provided after this warrant had been issued. *Id.* at 46: 2-5. As noted above, this confusion could have contributed to the misleading aspects of the affidavit regarding Bulletin Board A. After considering the presence of systemic errors in this investigation, and the likelihood of their recurrence in future investigations, the Court concludes that the importance of deterring misleading or unclear investigatory procedures is paramount. This importance outweighs the potential risks of suppressing the seized evidence.

The purpose of the exclusionary rule is "to deter some police misconduct and provide incentives for the law enforcement profession as a whole to conduct itself in accord with the Fourth Amendment." *United States v. Leon*, 468 U.S. 897, 918–19 (1984). Suppression is warranted where officers were dishonest or reckless in preparing their affidavit. *Id.* at 926. The inclusion of extensive information about the general criminal characteristics and tendencies of persons involved in child pornography crimes, despite the absence of any factual links to Defendant, was significantly misleading here.

Balancing the values upheld in our constitutional principles and fundamental rights against the importance of supporting sensitive law enforcement seeking to protect our most vulnerable victims is especially challenging. This Court found the wisdom imparted in the Second Circuit's decision in *United States v. Falso*, 544 F.3d 110 (2d Cir. 2008) helpful.

The *Falso* majority held that the good faith exception to the exclusionary rule applies most readily when the error is committed by the magistrate or court in issuing the warrant, not by the officers who executed it. *Id.* at 128–29. The dissenting opinion recognized that “it is perhaps somewhat disingenuous, after having gone to the [Magistrate Judge] with the paltry showing seen here, to suggest . . . that at bottom it was the [Judge] who made the error and the search and seizure are insulated because the officer's reliance on that error was objectively reasonable.” *Falso*, 544 F.3d at 136 (Jacobs, CJ., dissenting) (citing *United States v. Zimmerman*, 277 F.3d 426, 438 (3d Cir. 2002)). Where, as here, the executing officer is also the affiant—and the same officer who misled the issuing judge—the good faith exception to the exclusionary rule cannot apply, because it cannot be said that the executing officer reasonably relied on the search warrant. *See id.* at 134 (Jacobs, CJ., dissenting).

For the reasons provided, the Court is compelled to find that the warrant and affidavit here lacked sufficient probable cause to support the search of Defendant's residence. The good faith exception to the exclusionary rule is inapplicable because of the apparent reckless disregard for the truth evident during the process of making the warrant application, and because suppression here will likely result in the appreciable deterrence of potentially recurring constitutional violations that arise due to systemic investigatory issues.


IV. CONCLUSION

For the foregoing reasons, Mr. Reece's Motion to Suppress, ECF No. 21, is **GRANTED**.

The Clerk is **REQUESTED** to mail a copy of this Order to all attorneys of record.

IT IS SO ORDERED.

Norfolk, Virginia
March 1, 2017



Arenda L. Wright Allen
United States District Judge